REMARKS

The Examiner is thanked for the careful review of this application

Claims 1-24 are pending in the current application. Claims 1, 10, 11, 18, and 19 are independent claims. Claims 22-24 are added by this Amendment. Favorable reconsideration and allowance of the present patent application are respectfully requested in view of the foregoing amendments and the following remarks.

Claim Rejections under 35 U.S.C. §101

Claims 19-21 are rejected under 35 U.S.C. §101 for allegedly being directed to non-statutory subject matter.

By the present amendment, the preamble of independent claim 19 recites a "computer-readable storage medium." The Applicants respectfully submit that a "storage medium" does not read upon signals, but rather physical storage media such as hard drives, CD-ROMs, etc. (e.g., more examples are listed in Paragraph [0034]).

In view of the present Amendment to independent claim 19, the Applicants respectfully request that the Office withdraw this rejection.

Claim Rejections under 35 U.S.C. §103(a) over Shenfield in view of Kiiveri

Claims 1-10 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Publication No. 2004/0220998 ("Shenfield") in view of U.S. Publication No. 2005/0033969 ("Kiiveri"). The Applicants respectfully traverse this art ground of rejection.

Shenfield is directed to a system and method of building wireless component applications. The Office reads the claimed "computer platform" upon the application server. Independent claims 1 and 10 are directed to computer devices "having wireless communication capability," and not a more generic "computer device." As such, the Applicants submit that the computer devices of independent claims 1 and 10 cannot read on the application server 110 of Shenfield. With regard to the wireless communication devices actually disclosed by Shenfield (e.g., *mobile communication devices 100 as illustrated in Shenfield at FIG. 1, for example*), the

Applicant respectfully submit that Shenfield fails to disclose or suggest the remaining claim features under this interpretation of the claim language.

Further, the Applicants agree with the Office in that "Shenfield is silent in teaching a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol" (e.g., see Page 5 of the 12/24/2008 Office Action). However, the Office alleges that Kiivera cures this particular deficiency of Shenfield.

Kiivera is directed to a secure execution architecture, where secure environment hardware is kept physically separate from memory that stores potentially unsecure applications (*e.g., see* FIG. 1 of Kiivera). The CPU illustrated in FIG. 1 operates either in secure mode or unsecure mode (e.g., see FIG. 2 of Kiivera). The mode of the CPU is controlled by a security control register within the secure environment hardware, with respect to which Kiivera states that "[t]he purpose of the security control register is to give the CPU access to the secure environment, or preventing the CPU from accessing the secure environment, depending on the mode set in the register" (*e.g., see* [0025] of Kiivera). Kiivera states that "[i]n the secure mode, the processor has access to security related data located within the secure environment" (e.g., see [0030] of Kiivera), and that "if … unsecure mode is activated … [t]he secure environment is now inaccessible" (*e.g., see* [0032] of Kiivera).

With respect to FIG. 2 of Kiivera, Kiivera discloses that "signatures for the first protected application and operating system to be downloaded are checked", "[i]f the signatures are correct, the application and the operating system is downloaded into the secure environment RAM", and "if the signature check fails or if no signature is present, unsecure mode is activated and the non-verified application is loaded into the ASIC RAM located outside the secure environment" (*e.g., see* [0031]-[0032] of Kiivera).

As noted above, Kiivera teaches downloading verified applications to a secure environment RAM, and downloading non-verified applications to a non-secure RAM. However, Kiivera does not appear to disclose or suggest different mechanisms for downloading verified and non-verified applications. In the absence of such a teaching, the Applicants respectfully submit it is only reasonable to assume that the same mechanism is used for the downloading of verified and/or non-verified applications.

Accordingly, the Applicant respectfully submit that the combination of Shenfield and Kiivera cannot disclose or suggest "***the resident application environment*** configured to selectively download applications that comply with a predefined security protocol" and "***a download manager*** resident on the computer platform that is configured to selectively downloads applications that do not comply with the predefined security protocol" (Emphasis added) features, as recited in independent claim 1 and similarly recited in independent claim 10.

As such, claims 2-9, dependent upon independent claim 1, are likewise allowable over Shenfield in view of Kiiveri at least by virtue of their dependence upon the independent claims.

The Applicant respectfully requests that the Office withdraw this art grounds of rejection.

Allowance requested for newly added dependent claims 22-24

The Applicants further request an indication of allowance for newly added dependent claims 22-23. Dependent claim 22 recites "wherein the download manager exists within resident application environment and uses an existing application download interface" and "wherein the download manager further manages executing the downloaded application that does not comply with the predefined security protocol." In Kiivera, the secure environment hardware is disabled when non-verified applications are being executed. If the claimed "download manager exists within the resident application environment," and the Office reads the "resident application environment" upon the secure environment in Kiivera, then it would not be possible to execute the download manager and/or an execution of the downloaded application via the download manager during secure mode.

Dependent claim 23 recites "wherein the predefined security protocol includes an application validation requirement of the resident application environment." The Office has indicated that the "predefined security protocol" is being read upon the user name and password of the application server 110 in Shenfield (*e.g., see* Page 4 of the 12/24/2008 Office Action) to determine whether a download to a remote device is permitted. However, the username and password is a requirement of the application server 110, not the "resident application environment" which is within the computer device "having wireless communication capability" as claimed.

Dependent claim 24 recites "wherein the applications being downloaded by the resident application environment in compliance with the predefined security protocol and the applications being downloaded by the download manager in non-compliance with the predefined security protocol are both stored in the data store" (*e.g., see original dependent claim 6 for support of this Amendment, as well as the discussion of "data store", memory 20 and local database 22 within the Specification*). A review of FIG. 1 of Kiivera indicates that the verified and non-verified applications are stored in physically separate memory locations. Further, the Office has already admitted that Shenfield does not disclose the "download manager" feature, which is responsible for downloading and controlling a storage of the application. As such, the Applicants respectfully submit that the recitation of claim 24 is allowable over Shenfield and/or Kiivera.

Claim Rejections under 35 U.S.C. §102(e) over Kiiveri

Claims 11-21 are rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Publication No. 2005/0033969 ("Kiiveri"). The Applicants respectfully traverse this art ground of rejection.

The Applicants initially direct the Office to the Applicants' characterization of Kiivera in the preceding section. The Applicants incorporate the above-characterization of Kiivera for the sake of brevity. As noted above, Kiivera teaches downloading verified applications to a secure environment RAM, and downloading non-verified applications to a non-secure RAM. However, Kiivera does not appear to disclose or suggest "executing the application at the computer device with the download manager," as recited in independent claim 11 and similarly recited in independent claims 18 and 19.

The Office cites to Paragraph [0032] of Kiivera for allegedly disclosing this feature, but the only teaching in this section related to execution of the non-verified application is that "[w]hen boot is completed, this non-verified application is executed by the CPU." <u>This does not appear to disclose or suggest that the mechanism responsible for downloading the non-verified application is also responsible for its execution, as claimed</u>. In other words, a general execution of the non-verified application by the CPU in Kiivera does not imply that the non-verified application is executed by a download manager that was also used to download the non-verified application in the first place.

Accordingly, the Applicants respectfully submit that Kiivera cannot disclose or suggest "the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform" and "executing the application at the computer device with the download manager" features, as recited in independent claim 11 and similarly recited in independent claims 18 and 19.

As such, claims 12-17 and 20-21, dependent upon independent claims 11 and 19, respectively, are likewise allowable over Kiiveri at least by virtue of their dependence upon the independent claims.

The Applicants respectfully request that the Office withdraw this art grounds of rejection.

Reconsideration and issuance of the present application is respectfully requested.

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: March 20, 2009

By: /Fariba Yadegar-Bandari/

Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502